



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,303	08/30/2000	Douglas B. Moran	RECOP012	2514
21912	7590	06/15/2004	EXAMINER BAUM, RONALD	
VAN PELT & YI LLP 10050 N. FOOTHILL BLVD #200 CUPERTINO, CA 95014			ART UNIT 2136	PAPER NUMBER 9

DATE MAILED: 06/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/651,303

Applicant(s)

MORAN, DOUGLAS B.

Examiner

Ronald Baum

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 16 April 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1,2 and 4-23 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,2,4-23 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### DETAILED ACTION

1. This action is in reply to applicant's correspondence of 16 April 2004.
2. Claims 1,2,4-23 are pending for examination.
3. Claims 1,2,4-23 are rejected.

### *Specification*

4. The disclosure is objection dealing with various informalities is withdrawn.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1,2,4-23 are rejected under 35 U.S.C. 102(b) as being anticipated by Maloney et al, U.S. Patent 6,269,447 B1.
6. As per claim 1; "A system for detecting intrusions [ABSTRACT, col. 1, lines 20-31, 40-50, col. 2, lines 12-14, 34-40, col. 3, lines 1-14, col. 12, lines 21-35], comprising: an analysis engine [col. 2, lines 41-47, col. 3, lines 28-32, col. 4, lines 43-50, col. 5, lines 54-62, col. 7, lines 7-12]; and at least one sensor, configured to communicate with the analysis engine using at least one meta-protocol under which a 4-tuple is used to represent a data item to be sent to the analysis engine for analysis; wherein the 4-tuple represents the data item in a manner that enables the

Art Unit: 2136

analysis engine to receive and use the data item regardless of how the data item is represented and organized on a platform associated with the sensor [figure 2 (meta data reference, and network addressing/database entry referencing parameters), col. 1, lines 54-col. 2, line 10, col. 2, lines 16-33, 48-50 ('deriving generic structure' reference), col. 4, lines 15-22, 34-37, col. 5, lines 24-28, 39-52, 63-67, col. 6, lines 38-44, col. 8, lines 27-34, col. 9, lines 24-30, 47-50, 54-58, col. 11, lines 47-col. 12, line 2].”;

And further as per claim 22; “A method for detecting intrusions [This claim is the method of the apparatus (system) claim 1, and is rejected for the same reasons provided for the claim 1 rejection above], comprising the steps of: providing an analysis engine; providing at least one sensor; and defining a meta-protocol including a 4-tuple for communication between the analysis engine and the at least one sensor; wherein the 4-tuple represents a data item to be sent to the analysis engine for analysis in a manner that enables the analysis engine to receive and use the data item regardless of how the data item is represented and organized on a platform associated with the sensor.”;

And further as per claim 23; “A computer program product for detecting intrusions on a host [This claim is the embodied in software method of the method claim 22, and is rejected for the same reasons provided for the claim 22 rejection above], the computer program product being embodied in a computer readable medium having machine readable code embodied therein for performing the steps of: providing an analysis engine; providing at least one sensor; and defining a meta-protocol including a 4-tuple for communication between the analysis engine and the at least one sensor; wherein the 4-tuple represents a data item to be sent to the analysis engine for analysis in a manner that enables the analysis engine to receive and use the data item

Art Unit: 2136

regardless of how the data item is represented and organized on a platform associated with the sensor.”

7. Claim 2 ***additionally recites*** the limitations that “The system as recited in claim 1, wherein the meta-protocol includes a data packet, and the data packet includes the 4-tuple.” The teachings of Maloney et al (figure 2 (meta data reference, and network addressing/database entry referencing parameters)) suggest such limitations;
8. Claim 4 ***additionally recites*** the limitations that “The system as recited in claim 1, wherein the 4-tuple comprises a semantic type, data type, data type size, and value of the data item.” The teachings of Maloney et al (figure 2 (meta data reference, and network addressing/database entry referencing parameters), and figure 4 (i.e., the address, password, user, etc., parameters represent the equivalent)) suggest such limitations;
9. Claim 5 ***additionally recites*** the limitations that “The system as recited in claim. 4, wherein the analysis engine is configured to use the data item to detect an intrusion.” The teachings of Maloney et al (ABSTRACT, col. 1,lines 20-31,40-50, col. 2,lines 12-14,34-40, col. 3,lines 1-14, col. 12,lines 21-35) suggest such limitations;
10. Claim 6 ***additionally recites*** the limitations that “The system as recited in claim. 1, wherein the at least one sensor is configured to communicate with the analysis engine using a plurality of meta-protocols.” The teachings of Maloney et al (figure 2 (meta data reference, and network addressing/database entry referencing parameters), col. 1,lines 54-col. 2,line 10, col. 2,lines 16-33,48-50(‘deriving generic structure’ reference), col. 4,lines 15-22,34-37, col. 5,lines 24-28,39-52,63-67, col. 6,lines 38-44, col. 8,lines 27-34, col. 9,lines 24-30,47-50,54-58, col. 11,lines 47-col. 12,line 2) suggest such limitations;

Art Unit: 2136

11. Claim 7 ***additionally recites*** the limitations that “The system as recited in claims 6, wherein each of the plurality of meta-protocols includes a 4-tuple.” The teachings of Maloney et al (figure 2 (meta data reference, and network addressing/database entry referencing parameters), col. 1, lines 54-col. 2, line 10, col. 2, lines 16-33, 48-50 (‘deriving generic structure’ reference), col. 4, lines 15-22, 34-37, col. 5, lines 24-28, 39-52, 63-67, col. 6, lines 38-44, col. 8, lines 27-34, col. 9, lines 24-30, 47-50, 54-58, col. 11, lines 47-col. 12, line 2) suggest such limitations;
12. Claim 8 ***additionally recites*** the limitations that “The system as recited in claim 6, wherein the analysis engine is configured to invoke the at least one sensor and specify a set of meta-protocols supported by the analysis engine, and wherein the at least one sensor is configured to select a meta-protocol from the set.” The teachings of Maloney et al (col. 8, lines 19-26, col. 5, lines 24-30 (such that the configuration of the system would inherently encompass configuration of the sensor subsystem, such as the communications protocols (data and meta data levels), col. 8, lines 34-40, col. 9, lines 55-60) suggest such limitations;
13. Claim 9 ***additionally recites*** the limitations that “The system as recited in claim 8, wherein the set is a null set, and the at least one sensor is configured to use a default protocol.” The teachings of Maloney et al (col. 8, lines 19-26, col. 5, lines 24-30 (such that the configuration of the system would inherently encompass configuration of the sensor subsystem, such as the communications protocols (data and meta data levels, including active, initialized, default (i.e., null set specified), and degraded states (i.e., figure 3, ‘promiscuous mode’ reference), col. 8, lines 34-40, col. 9, lines 55-60) suggest such limitations;
14. Claim 10 ***additionally recites*** the limitations that “The system as recited in claim 7, wherein the analysis engine is configured to specify a set of semantic codes representing data

Art Unit: 2136

being requested by the analysis engine.” The teachings of Maloney et al (figure 2 (meta data reference, and network addressing/database entry referencing parameters), col. 1, lines 54-col. 2, line 10, col. 2, lines 16-33, 48-50 (‘deriving generic structure’ reference), col. 4, lines 15-22, 34-37, col. 5, lines 24-28, 39-52, 63-67, col. 6, lines 38-44, col. 8, lines 27-34, col. 9, lines 24-30, 47-50, 54-58, col. 11, lines 47-col. 12, line 2, figure 4 references to the various applications, and password types (i.e., FTP versus WWW versus POP3, etc.)) suggest such limitations;

15. Claim 11 ***additionally recites*** the limitations that “The system as recited in claim 10, wherein the at least one sensor is configured to supply data associated with the semantic codes, and wherein the at least one sensor further supplies data not associated with the semantic codes.” The teachings of Maloney et al (col. 8, lines 19-26, col. 5, lines 24-30 (such that the configuration of the system would inherently encompass configuration of the sensor subsystem, such as the communications protocols (data and meta data levels, including active, initialized, default (i.e., null set specified), and degraded states (i.e., figure 3, ‘promiscuous mode’ reference would encompass allowing data transfer of specified and *non-specified types (i.e., semantic specification)* of data as per a given specified or selected (meta) protocol), col. 8, lines 34-40, col. 9, lines 8-14, 55-60) suggest such limitations;

16. Claim 12 ***additionally recites*** the limitations that “The system as recited in claim 11, wherein the analysis engine is configured to disregard the data not associated with the semantic codes.” The teachings of Maloney et al (col. 8, lines 19-26, col. 5, lines 24-30 (such that the configuration of the system would inherently encompass configuration of the sensor subsystem, such as the communications protocols (data and meta data levels, including active, initialized, default (i.e., null set specified), and degraded states (i.e., figure 3, ‘promiscuous mode’ reference

Art Unit: 2136

would encompass allowing data transfer of specified and non-specified types (i.e., semantic specification) of data as per a given specified or selected (meta) protocol. Further, as per figures 2,3,5 the visual representation of said *disregarded data* (as well as 'regarded' data) would encompass the associated (*disregarded*) data), col. 8,lines 34-40, col. 9,lines 8-14,55-60) suggest such limitations;

17. Claim 13 ***additionally recites*** the limitations that "The system as recited in claim 10, wherein the set of semantic codes is a null set, and the at least one sensor is configured to use a default set of semantic codes." The teachings of Maloney et al (col. 8,lines 19-26, col. 5,lines 24-30 (such that the configuration of the system would inherently encompass configuration of the sensor subsystem, such as the communications protocols (*semantic (i.e., type)* of data, the actual data, and meta data levels, including active, initialized, default (i.e., null set specified), and degraded states (i.e., figure 3, 'promiscuous mode' reference), col. 8,lines 34-40, col. 9,lines 55-60) suggest such limitations;

18. Claim 14 ***additionally recites*** the limitations that "The system as recited in claim 1, wherein the analysis engine is located on a first host and an instance of the at least one sensor is located on a second host apart from the first host." The teachings of Maloney et al (figure 2, and associated description, col. 2,lines 15-33) suggest such limitations;

19. Claim 15 ***additionally recites*** the limitations that "The system as recited in claim, 14, comprising a second instance of the at least one sensor, wherein the second instance is located on a host apart from the second host." The teachings of Maloney et al (figure 2, and associated description, col. 2,lines 15-33, col. 5,lines 34-38, col. 6,lines 33-38, col. 7,lines 22-24) suggest such limitations;

Art Unit: 2136

20. Claim 16 ***additionally recites*** the limitations that “The system as recited in claim 1, wherein the at least one sensor includes a sensor collector in communication with the analysis engine.”. The teachings of Maloney et al (col. 8, lines 19-26, col. 5, lines 24-30 (such that the configuration of the system would inherently encompass configuration of the sensor subsystem, such as the communications protocols (data and meta data levels), and sensor routing of collection functions (i.e., figure 3), col. 8, lines 34-40, col. 9, lines 55-60) suggest such limitations;

21. Claim 17 ***additionally recites*** the limitations that “The system as recited in claim 1, further comprising a sensor collector disposed in a communication path between the analysis engine and the at least one sensor.”. The teachings of Maloney et al (col. 8, lines 19-26, col. 5, lines 24-30 (such that the configuration of the system would inherently encompass configuration of the sensor subsystem, such as the communications protocols (data and meta data levels), and sensor routing of collection functions (i.e., figure 3, configuration of *sensor manager*), col. 8, lines 34-40, col. 9, lines 55-60) suggest such limitations;

22. Claim 18 ***additionally recites*** the limitations that “The system as recited in claim 1, wherein the analysis engine is configured to load a rule set while the analysis engine is in operation.”. The teachings of Maloney et al (col. 4, lines 20-33, col. 5, lines 7-17, 33-53, col. 6, lines 45-59, col. 7, lines 7-34, col. 8, lines 34-50, col. 9, lines 9-14, 37-41, col. 11, lines 1-5, col. 12, lines 21-34) suggest such limitations;

23. Claim 19 ***additionally recites*** the limitations that “The system as recited in claim 1, further comprising a second sensor, and wherein the analysis engine is configured to load a rule set for the second sensor while the analysis engine is in operation.”. The teachings of Maloney

Art Unit: 2136

et al (col. 4,lines 20-33, col. 5,lines 7-17,33-53, col. 6,lines 45-59, col. 7,lines 7-34, col. 8,lines 34-50, col. 9,lines 9-14,37-41, col. 11,lines 1-5, col. 12,lines 21-34, figure 2, and associated description, col. 2,lines 15-33, col. 6,lines 33-38) suggest such limitations;

24. Claim 20 ***additionally recites*** the limitations that “The system as recited in claim 19, wherein the rule set is configured to specify interactions of data from the second sensor with data from the at least one sensor.”. The teachings of Maloney et al (col. 4,lines 20-33, col. 5,lines 7-17,33-53, col. 6,lines 45-59, col. 7,lines 7-34, col. 8,lines 34-50, col. 9,lines 9-14,37-41, col. 11,lines 1-5, col. 12,lines 21-34, figure 2, and associated description, col. 2,lines 15-33, col. 6,lines 33-38) suggest such limitations;

25. Claim 21 ***additionally recites*** the limitations that “The system as recited in claims 20, wherein the analysis engine is configured to ignore rules in the rule set that specify data not supplied by any sensor.”. The teachings of Maloney et al (col. 4,lines 20-33, col. 5,lines 7-17,33-53, col. 6,lines 45-59, col. 7,lines 7-34, col. 8,lines 34-50, col. 9,lines 9-14,37-60, col. 11,lines 1-5, col. 12,lines 21-34, figure 2, and associated description, col. 2,lines 15-33, col. 6,lines 33-38,mmmm, col. 8,lines 19-26, col. 5,lines 24-30 (such that the configuration of the system would inherently encompass configuration of the sensor subsystem, such as the communications protocols, and *rules criteria* (data and meta data levels, including active, initialized, default (i.e., null set specified), and degraded states (i.e., figure 3, ‘promiscuous mode’ reference would encompass allowing data transfer and *the rules governing such transfer*, of specified and non-specified types (i.e., semantic specification) of data as per a given specified or selected (meta) protocol. Further, as per figures 2,3,5 the visual representation of said

Art Unit: 2136

*disregarded data* (as well as 'regarded' data) would encompass the associated (*disregarded data*)) suggest such limitations;

***Response to Amendment***

26. As per applicant's argument concerning Maloney et al not teaching or specifically not suggesting the claim elements involved with using a "4-tuple" to represent the data from the sensor to the analysis engine, the examiner has fully considered the arguments and finds them not to be persuasive. The qualifier "suggests" also encompasses the interpretation of the claim language as *broadly interpreted by the examiner*, which would be proper under 35 USC 102 (and '103 for that matter).

Further, the Maloney et al "generic structure", as *broadly interpreted by the examiner*, could encompass data structures as simple as 8 bit byte data, or as complex as instantiated objects of any arbitrarily defined class, such that the "4-tuple" as *recited in the claim language* in claims 1,22 and 23, would be taught or suggested by the Maloney et al reference.

27. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

Art Unit: 2136

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.


***Conclusion***

28. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu, can be reached at (703) 305-4393. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum

Patent Examiner

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100